Digital C4I Interoperability: The EM Protection Issue

Robert Pfeffer
U.S. Army Nuclear and Chemical Agency
ATTN: ATNA-NU (R. Pfeffer)
7150 Heller Loop Suite 101
Springfield, VA 22150-3198

Abstract

In this paper, a unified protection methodology is applied to a digital mobile C4I platform subjected to several human-generated and nature-generated EM environments and effects. The unclassified values for self-induced electromagnetic interference (EMI), EM radiation (EMR), electrostatic discharge (ESD), near-strike lightning, and high-altitude EM pulse (HEMP) came from MIL-STD-464 and several commercial standards. By applying this methodology the EM protection requirements were estimated to be 70 dB enclosure port protection for frequencies between 100 MHz and 5 GHz, and 80 dB penetration port protection on the phone line for frequencies dependent upon the length of the phone line used. This EM protection strategy is both useful and cost effective to coalition forces, since validation testing and maintenance/surveillance testing to meet international standards reduce to simple, low-cost shield and penetration protection tests that can be conducted anywhere, even with the system operating. The application of this protection approach in the original system circuit design significantly reduces the number of breadboard and brassboard tests. Such protection also allows component replacement within the barrier, once the new component immunity level has been measured.

1. Introduction

The end of the Cold War brought many changes to the military. In the U.S., top-down and bottom-up reviews concluded the threat has changed but not gone away. Global warfare is now less likely than regional war, and these wars will likely be fought with coalition forces. Joint operations among equal partners, such as Desert Storm and recent peacekeeping actions in Bosnia-Herzegovina and Kosovo, are expected to be more the rule than the exception in the first few decades of the new millennium. To address the regional threat more effectively, the U.S. military made significant changes in several areas: in the acquisition system, in troop strength and base relocation/closures, and in budgetary matters. This paper begins with a discussion on acquisition changes that have made a significant impact on the way the U.S. Army approaches system EM protection. The paper then outlines a unified approach to EM protection that is consistent with these changes.

1.1 *Interoperable C4I*

Integral to the success of joint allied operations will be the use of advanced technology, interoperable digital command, control, communications, computer and intelligence (C4I)

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2000		**00-00-2000 to 00-00-2000**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Digital C4I Interoperability: The EM Protection Issue	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Army Nuclear and Chemical Agency,ATTNL ATNA-NU,7150 Heller Loop Suite 101,Springfield,VA,22150-3198**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
5th International Command and Control Research and Technology Symposium

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**11**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

systems to coordinate a wide range of critical military inter-force and intra-force actions. In addition, the next-generation C4I will also be used for surveillance and reconnaissance. Collectively, these systems are sometimes referred to as C4ISR, although they will be called C4I in this paper. They will be few in number and probably nation-unique; however, all will manipulate enormous quantities of data continuously and in real time, and, because they are digital, could be lightweight and small in size, and will have very low operating voltages (1.5 volts or less). If these C4I system building blocks consist of unprotected commercial-off-the-shelf (COTS) components, they could be extremely sensitive to battlefield conditions (nuclear, conventional). Enemy/terrorist forces will then recognize these mission-critical, digital C4I systems as high-priority targets.

1.2 *Asymmetric EM Threats*

One of the projected asymmetric threats against these systems will likely be electromagnetic (EM) in origin. Fieldable EM generators already exist that can upset or destroy present-generation digital electronics. For example, electronic warfare jamming technology is already available to most nations. Radio-frequency (RF) weapons, such as high-power microwave and wideband weapons, could soon be deployed in the field to jam or damage electronics, and high-altitude EM pulse (HEMP) is already a battlefield-wide threat. This paper addresses a consistent digital C4I protection methodology against a wide range of wideband and narrowband EM environments and effects, including RF and HEMP, which can be adopted by joint forces to protect their critical C4I systems. It accounts for differences in digital circuit design and can be applied to meet any set of commercial and/or military EM requirements.

2. Relevant Military Acquisition Issues

One of the most significant changes to the military during the transition from Cold War to post-Cold War has taken place in the system acquisition process. The reduced threat of war to the homeland has led to a significant change to the process, a change intended to further reduce acquisition costs while still benefiting from commercial state-of-the-art technology. The process is evolving still, but we already see irrevocable changes from the days of Legacy (Cold War) equipment development.

2.1 *Cost*

By far the single, most important acquisition issue today is cost. Virtually all tradeoff decisions are made based on cost. Reduced defense budgets and the authority given to program/project managers to better control their acquisition costs allow them to “tradeoff” requirements that could increase costs, including costs associated with increased acquisition times. Operational requirements, such as frequency band and security requirements, are generally not considered tradeoff requirements. Survivability requirements, however, are tradeoff candidates, especially if the cost to meet them is high and the occurrence probability is low. Protection against a direct lightning strike might also be a tradeoff candidate. The challenge is to find an affordable protection method that maximizes protection to many threats.

The problem with reducing C4I costs without the proper risk analysis is that C4I networks could be upset or catastrophically damaged by EM signals just above normal operating levels. By looking at the most important EM environments (international standards) to which all nations subscribe and then obtaining the coupled signals onto mission-critical subsystems, including COTS, system developers can estimate protection costs before conducting any breadboard tests. This is especially important, since some or all protection can be provided by existing government-furnished equipment at low or no additional cost. An example is the use of metallic-walled shelters as the primary shield for internal C4I systems, and controlling shield penetrations (e.g., EMC doors, gasketing signal and power line apertures). Such an approach supports interoperability in that it predicts whatever minimum protection is necessary to assure different nations C4I survive the same international threats without dictating what electronics or what level of protection to use.

2.2 *Frequency Allocation*

Another C4I acquisition issue is frequency allocation. Recent sales of traditional military frequencies to the public have significantly reduced military frequency bands. Unfriendly forces can use this knowledge to interfere with military C4I more effectively. For example, by knowing the relatively narrowband frequency allocation for a particular unprotected C4I network, one can develop in-band techniques to upset or otherwise compromise the mission. To counter this threat, system designers must implement an affordable and flexible EM protection approach that not only protects present-generation COTS equipment but also allows them to be replaced with the next-generation COTS.

3. EM Protection Unification

A complete description of the unified approach to EM protection was given in a paper[1] presented at the 4th International Command and Control Research and Technology Symposium, Nasby Slott, Sweden. A brief description of the same EM protection philosophy and methodology is given below and is illustrated in Figure 1.

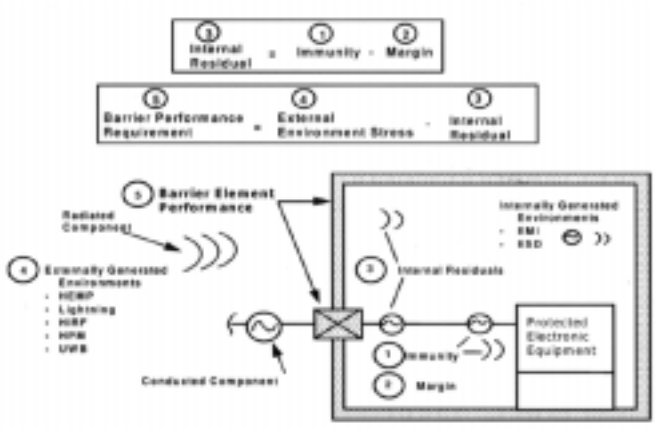


Figure 1. Typical Protection Concept Keyed to Allocation Equations

[1] Pfeffer, R, et al, A Unified Approach to Electromagnetic Protection, 4th International Command and Control Research and Technology Symposium, Nasby Slott, Sweden, 14-16 September, 1998.

3.1 *Barrier*

In the most general case, an EM barrier consists of many shields and shield penetrations. Figure 2 illustrates typical examples of a system EM barrier. In many military systems, the EM barrier reduces to a single shield with several penetrations.

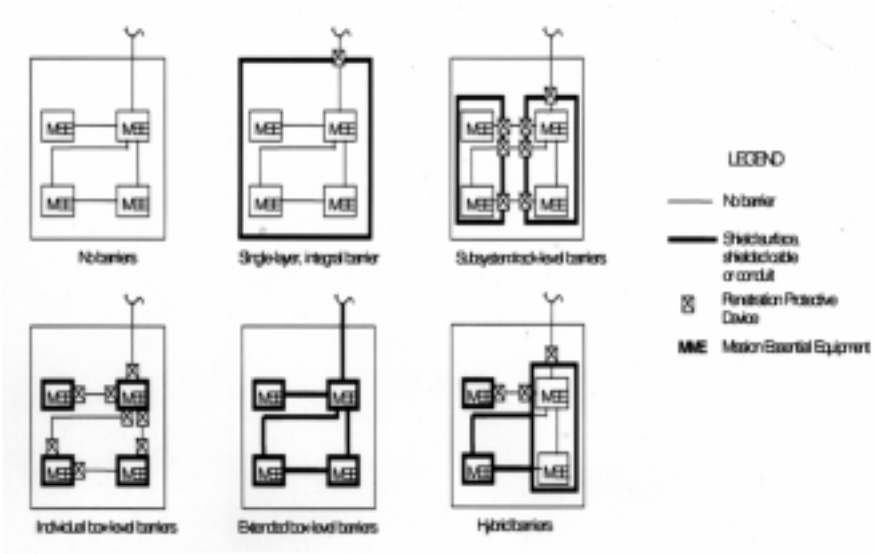


Figure 2. Typical EM Barriers

3.2 *Immunity*

Immunity is the inherent protection level of an electronic package as measured by a standard, box-level test or tests. It can also be thought of as the inverse of package sensitivity. Thus, the minimum immunity bound is the onset of upset/failure. For digital C4I, the onset of upset generally establishes the minimum immunity bound. Existing military and/or civilian EM standards are used to determine the immunity bounds. Immunities can also be customized to meet specific system requirements. MIL-STD-461E[2] is a military standard that contains both conducted and radiated immunity requirements for different types of equipment installed on platforms. The IEC-1000-4/EN61000-6 series is a civilian series of standards that addresses radiated and conducted immunities for various applications. The existing immunity standards may need to be augmented (tailored) for specific coverage (e.g., to cover frequency ranges or levels not covered by the commercial or military standards chosen) depending on specific system requirements. External radiated or conducted environment system-level immunity tests are described in MIL-STD 464, although there are other commercial box and system-level tests. For this paper, most immunity testing will be those described in MIL-STD- 461E and MIL-STD-464.

3.3 *Margin*

System designers use margin as a way to account for immunity variations, test uncertainties, operational degradation, and risk. The lower limit on margin is typically 6 dB. The upper range can approach 40 dB. Only the highest-value targets should include this much margin allocation,

[2] MIL-STD-461C, D and MIL-STD-462 have been combined and replaced with MIL-STD-461E.

as extra margin can result in significant cost and operational performance impacts. For this example, the margin will be 6 dB for each equipment unit and all frequencies.

3.4 *Internal Residual*

Figure 1, equation 1, shows that the internal residual is defined as the difference between the immunity and the margin, each term expressed in dB. There are conducted and radiated internal residuals. Conducted internal residuals are the residuals allowed on the "clean" side of the penetration protective devices. In general, conducted internal residuals will be different for the different classes of penetration ports. For example, power conductor internal residuals will differ from signal/data conductor residuals. Radiated internal residuals are the residual externally generated fields that have penetrated the electromagnetic shield.

Internal residuals are usually dominated by the externally generated environment leakage through the barrier. In some cases, internally generated environments dominate the external environment residuals. For example, ESD radiated fields can be very large. In these cases, the internally generated environments will control the residuals.

3.5 *Protection*

The minimum EM protection required of the shield enclosure and the penetration port controls is the difference between the external stress and the internal residual. Figure 3 illustrates the case for a barrier consisting of a simple shield and a single shield penetration. Note the calculations are repeated for each immunity and each environment.

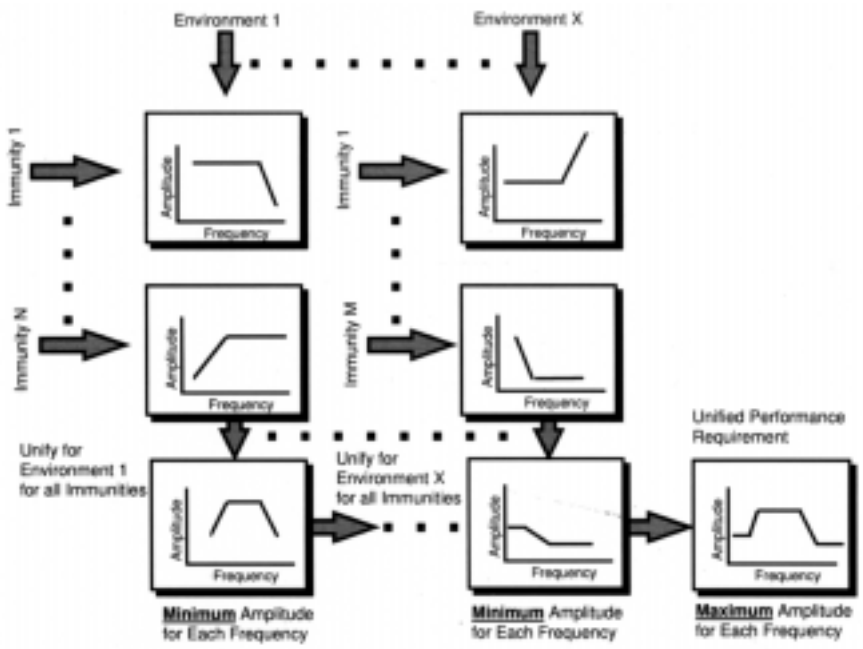
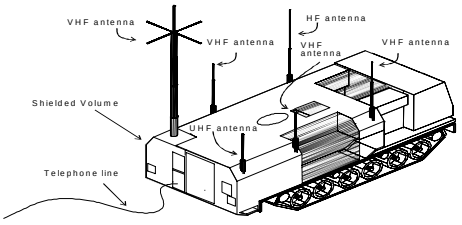


Figure 3. General Approach to Deriving Performance Requirements

3.6 *System Test Validation*

Some validation testing is necessary to indicate a real field-configured system meets the required standards. These tests, however, can become very simple shield and penetration control tests when the design engineer uses the protection approach described above.

4. System Application



The digital C4I system under consideration is a light-armored, tracked vehicle containing several electronic subsystems. These electronic subsystems typically share a common ground and internal power source. Self-compatibility is an operational operate through requirement, as is the EMRO environment. In addition, there are several electromagnetic environmental effects (E3) survivability requirements. For this example, the E3 survivability requirements are for HEMP, EMR hazard (EMRH), near-strike lightning, and electrostatic discharge (ESD).

4.1 *Threat Definition*

It is common practice to identify commercial standards wherever possible. For this example, however, we simplify the discussion by referencing requirements to MIL-STD-464.

4.2 *System EM Characterization*

To minimize protection costs, an attempt is made to use the existing system barrier to provide the necessary minimum EM protection. The system's light armor will be the primary shield, and the various penetration ports through that shield will be controlled. Penetration ports include electrical ports (antennas, signal/phone lines) and physical ports (personnel entry ways, apertures for air-conditioning, NBC ports). Given the E3 environments represented by the standards stated above, calculations are made to determine the minimum protection requirements of the shield and the penetration ports.

4.3 *Enclosure Port Protection Requirement*

Because the system and the E3 standards are the same as the example in reference 1, and because the system has an operate through requirement, the minimum enclosure port protection requirement is 70 dB rather than the more usual 40-60 dB. It is the result of applying Figure 3 for each of the four environments and then taking the maximum (or worst case) envelope.

4.4 *Penetration Port Protection Requirements*

Reference 1also calculated the minimum penetration port protection level for a monopole antenna. The process is the same for other antennae mounted on the vehicle and will not be repeated here. This paper calculates the phone line minimum penetration port protection level for both narrowband and transient cases.

The first step is to develop a simple equivalent circuit with an assumed source impedance of 220 ohms. The model is then used to calculate the phone line broadband response to a unit impulse field (Figure 4).

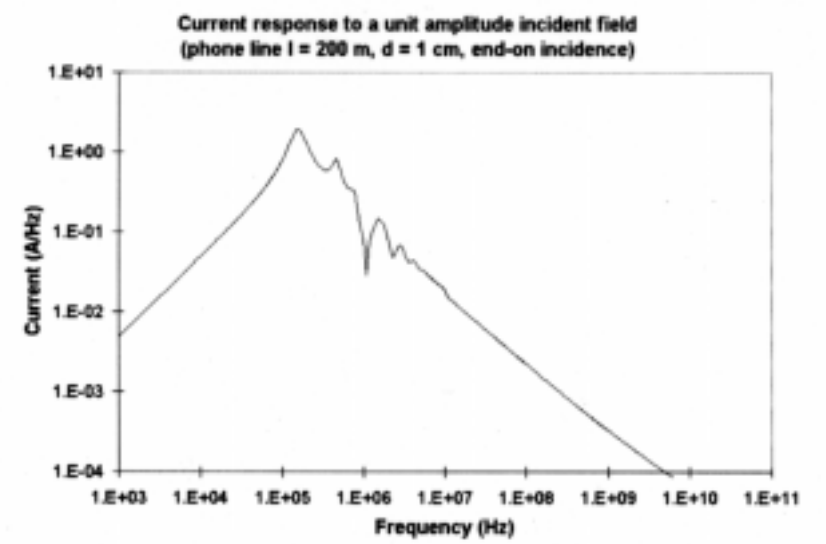


Figure 4. Broadband Response of the Phone Line to a Unit Amplitude Field

The conducted environments for each radiated environment is then obtained by combining the impulse response with each of the various incident fields. Figure 5 identifies the phone line transient current response to lightning and HEMP fields for two different line lengths.

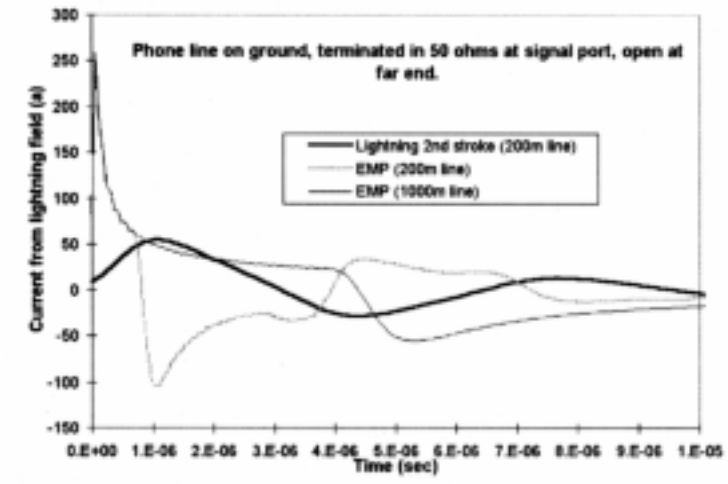


Figure 5. Phone Line Transient Response

The broadband current response of the phone line is plotted versus frequency in Figure 6.

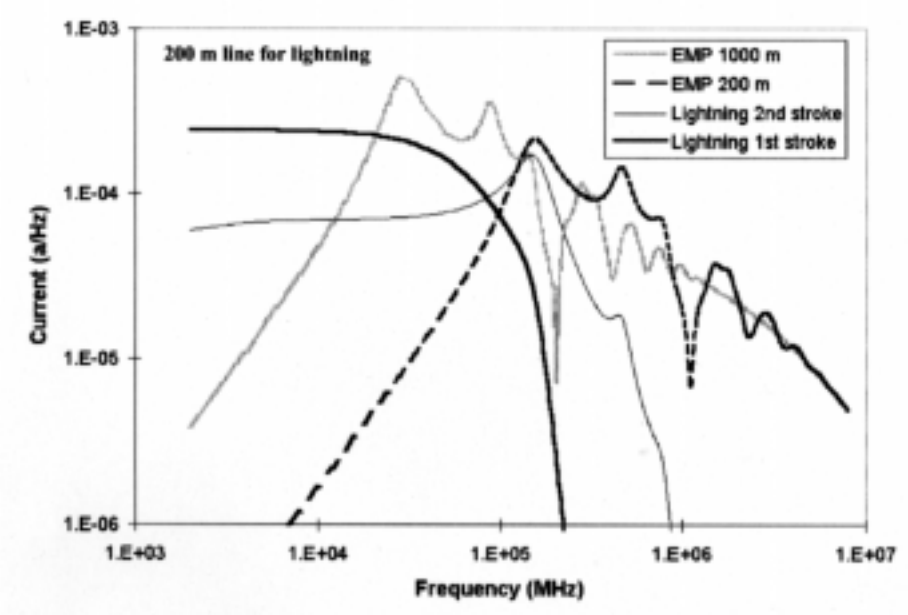


Figure 6. Phone Line Broadband Response

This same procedure is used to obtain the narrowband results. Figure 7 is a plot of the phone line narrowband response as a function of frequency.

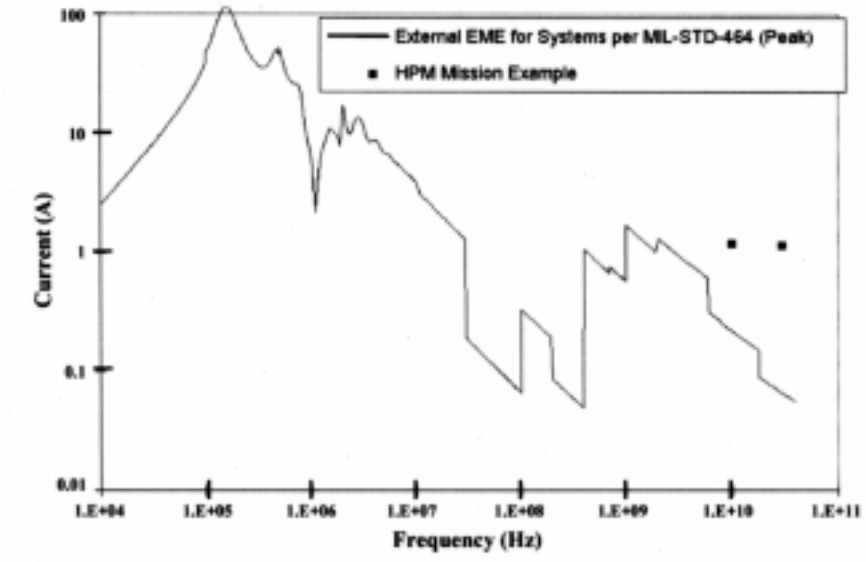


Figure 7. Frequency Domain Plot of Narrowband Response

Once the conducted environments have been obtained, the procedure for establishing the minimum protection performance requirement begins with the steps mentioned in Section 3. Note these requirements are expressed as dB attenuation plotted as a function of frequency.

Phone line unified protection requirements for the transient conducted environments are plotted in Figure 8, and narrowband conducted environments are plotted in the frequency domain in Figure 9.

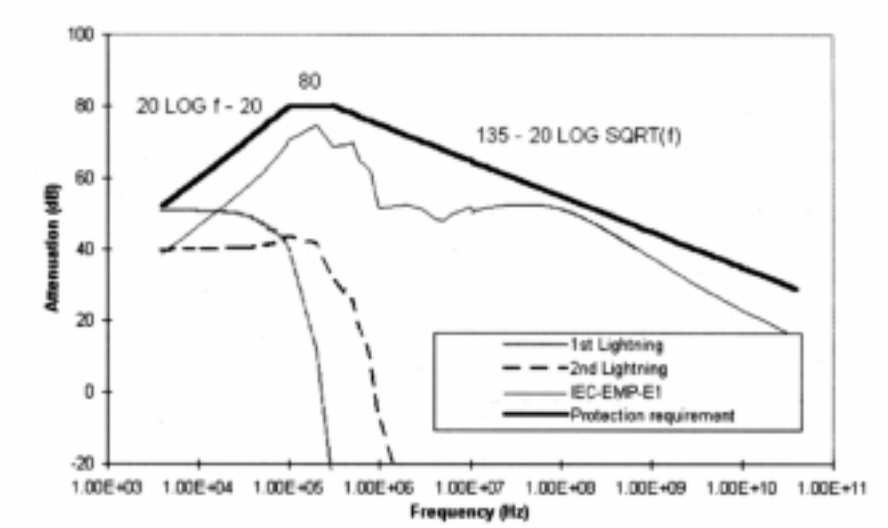


Figure 8. Unified Protection Requirements for Transient Conducted Environments

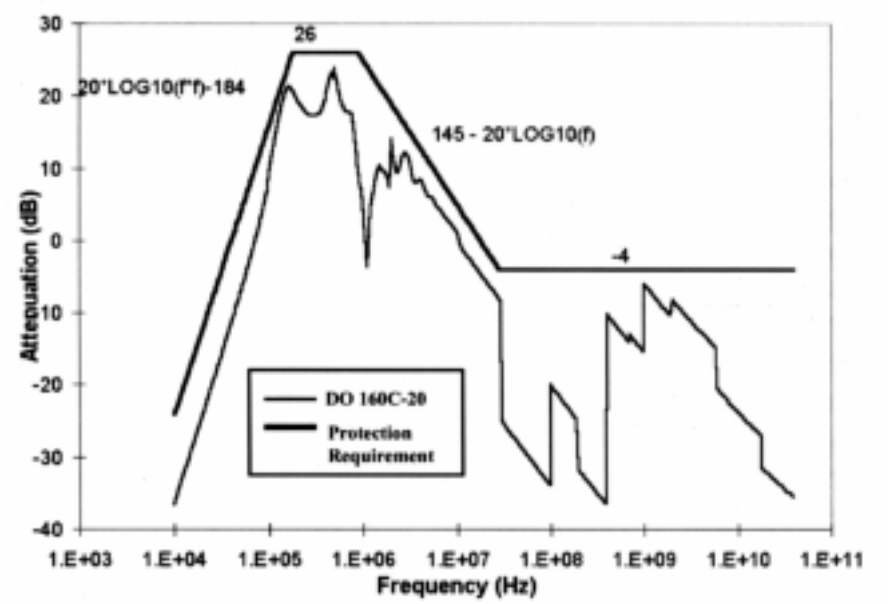


Figure 9. Unified Protection Requirements for Narrowband Conducted Environments

4.5 *Test Validation*

Now that the minimum enclosure (shield) and all penetration port protection levels have been established, specific measures can be taken to design-in protection. When this protection is provided at the shield and penetration ports, the design engineer has maximum flexibility to locate the electronics anywhere inside the barrier and to simplify the test procedure, especially

when requirements overlap. For the system under discussion, HEMP immunity testing is satisfied when shield and penetration port tests are done for EMI/EMC, since there is an operate through requirement for EMI/EMC and not for HEMP. A system-level validation test can then reduce to simple barrier penetration and shielding effectiveness validation tests. Table 1 defines the appropriate immunity tests and system-level tests required of the system.

Table 1. Typical Specification/Applicability Table for Electronics in a Barrier

Environment / Design Test Requirements	EMI/EMC	EMR		EMP	ESD			Nearby Lightning
		EMRO	EMRH		INT.	EXT.	Safety	
CE102 Power Line	✕							
CE106 Antenna Line	✕							
CS101 Power Line	✕							★
CS103 Antenna Line; Intermodulation	✕	✕						
CS104 Antenna Line; Signal Rejection	✕	✕						
CS105 Antenna Line; Cross Modulation	✓	✕						
CS114 Bulk Cable Current	✕	✕		★				
CS115 Bulk Cable Impulse	✓	✕	□	★				★
CS116 Dumped Sinusoid Transients	✕			★				★
RE102 Rad Emissions	✕							
RS103 Rad Susceptibility; Operate Limits	✕	✕						
HEMP Free Field External to Enclosure				★				
RS103 Rad Susceptibility; Safety Limits			□					
IEC 801-2, Level 4 Internal ESD					✕			
MIL-STD 331B External ESD						✕		
MIL-STD 331B ESD Safety							□	
EMRH Tests Shipping / Storage			□					
Life-cycle Control & Maintenance	✓	✓	✓	✓	✓	✓	✓	✓

Notes: 1. ✕ Indicates operate through requirement
2. ★ Indicates movement capability required within 3 minutes and all other mission critical function capability required within 10 minutes after environmental exposure
3. □ Indicates subsystem equipment must not present a hazard to personnel when environment applied
4. ✓ Applicable

5. Conclusions

The use of a unified approach to EM protection provides system developers with a powerful technique for reducing EM protection costs without compromising EM protection. For digital C4I systems, including those supporting coalition operations, the approach accommodates the use of government-furnished equipment and/or COTS, works with any commercial or military

standards, and addresses all military frequency bands. In the example, the digital circuits are sensitive to E3 and they have an operate through requirement; hence, the low immunity levels and high barrier performance requirements.

6. References

[MIL-STD-461E, 1999] *Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment*, U.S. Department of Defense Interface Standard, U.S. Department of Defense, 1999

[MIL-STD-464, 1998] *Interface Standard for Systems Electromagnetic Environmental Effects Requirements*, U.S. Department of Defense Interface Standard, U.S. Department of Defense, 1998